

THE WEIGHT DISTRIBUTIONS OF A CLASS OF CYCLIC CODES II

MAOSHENG XIONG

ABSTRACT. Recently, the weight distributions of the duals of the cyclic codes with two zeros have been obtained for several cases in [10, 5, 15, 16]. In this paper we use the method developed in [16] to solve one more special case. We make extensive use of standard tools in number theory such as characters of finite fields, the Gauss sums and the Jacobi sums. The problem of finding the weight distribution is transformed into a problem of evaluating certain character sums over finite fields, which turns out to be associated with counting the number of points on some elliptic curves over finite fields. We also treat the special case that the characteristic of the finite field is 2.

1. INTRODUCTION

Denote by $\text{GF}(q)$ the finite field of order q , where $q = p^s$, s is a positive integer and p is a prime number. An $[n, k, d]$ -linear code \mathcal{C} over $\text{GF}(q)$ is a k -dimensional subspace of $\text{GF}(q)^n$ with minimum distance d . If, in addition, \mathcal{C} satisfies the condition that $(c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$ whenever $(c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in \mathcal{C}$, then \mathcal{C} is a cyclic code. Let A_i denote the number of codewords with Hamming weight i in \mathcal{C} . The weight enumerator of \mathcal{C} is defined by

$$1 + A_1x + A_2x^2 + \cdots + A_nx^n.$$

2000 *Mathematics Subject Classification.* 94B15, 11T71, 11T24.

Key words and phrases. Cyclic codes, weight distribution, elliptic curves, character sums.

The author was supported by the Research Grants Council of Hong Kong under Project Nos. RGC606211 and DAG11SC02.

The sequence $(1, A_1, \dots, A_n)$ is called the weight distribution of \mathcal{C} . In coding theory it is often desirable to know the weight distribution of a code because it contains a lot of important information, for example, it can be used to estimate the error correcting capability and the probability of error detection and correction with respect to some algorithms. This is quite useful in practice. Many important families of cyclic codes have been studied extensively in the literature, so have their various properties. However the weight distributions are difficult to obtain in general and they are known only for a few special families.

Given a positive integer m , let $r = q^m$, and α be a generator of the multiplicative group $\text{GF}(r)^* := \text{GF}(r) - \{0\}$. Let h be a positive factor of $q - 1$ and $1 < e$ be an integer such that $e \mid \gcd(q - 1, hm)$. We define

$$(1) \quad g = \alpha^{(q-1)/h}, n = \frac{h(r-1)}{q-1}, \beta = \alpha^{(r-1)/e}, N = \gcd\left(\frac{r-1}{q-1}, \frac{e(q-1)}{h}\right).$$

It is clear that the order of g is n and $(g\beta)^n = 1$. Refining an argument from [10], we will prove later that the minimal polynomials of g^{-1} and $(\beta g)^{-1}$ are distinct over $\text{GF}(q)$, hence their product is a factor of $x^n - 1$, except when $q = 3, h = 1, e = m = 2$. We remark that the conditions here are slightly more general than those in [10, 5, 16] (and in several other references), which require that $e \mid h$. This consideration is inspired by an anonymous referee and actually provides more flexibility.

Define the cyclic code over $\text{GF}(q)$ by

$$(2) \quad \mathcal{C}_{(q,m,h,e)} = \{\mathbf{c}_{(a,b)} : a, b \in \text{GF}(r)\},$$

where the codeword $\mathbf{c}_{(a,b)}$ is give by

$$(3) \quad \mathbf{c}_{(a,b)} := \left(\text{Tr} \left(ag^i + b(\beta g)^i \right) \right)_{i=0}^{n-1}.$$

Here for simplicity Tr is the trace function from $\text{GF}(r)$ to $\text{GF}(q)$.

The code $\mathcal{C}_{(q,m,h,e)}$ has been an interesting subject of study for a long time. For example, when $h = q - 1$, the code $\mathcal{C}_{(q,m,h,e)}$ is the dual of a primitive cyclic linear code with two zeros; such codes have been studied extensively (see for example [1, 2, 3, 4, 8, 9, 11, 12, 14, 17]). In general the dimension of $\mathcal{C}_{(q,m,h,e)}$ is $2m$, but determining the weight distribution is very difficult. However, in certain special cases the weight distribution is known. We summarize these cases below.

- 1) $e > 1$ and $N = 1$ ([10]);
- 2) $e = 2$ and $N = 2$ ([10]);
- 3) $e = 2$ and $N = 3$ ([5]);
- 4) $e = 2$ and $p^j + 1 \equiv 0 \pmod{N}$, where j is a positive integer ([5]);
- 5) $e = 3$ and $N = 2$ ([15]);
- 6) $e = 4$ and $N = 2$ ([16]).

In this paper we compute the weight distribution for one more case $e = N = 3$. As it turns out, if $p \equiv 1 \pmod{3}$, the number of distinct nonzero weights in the codes is 12 or 13, the shortest code in the family has length $\frac{p^3-1}{p-1}$ over $\text{GF}(p)$. On the other hand, if $p \equiv 2 \pmod{3}$, then the number of distinct nonzero weights is 5 or 6, and the shortest code in the family has length $\frac{p^6-1}{p^2-1}$ over $\text{GF}(p^2)$. The dimension is always $2m$ where $3|m$, so the smallest dimension is 6. We have computed several examples for relatively small parameters by Magma, and thanks to the referee's suggestions, we also compare them with the best existing codes from Markus Grassl's table (<http://www.codetables.de/>). It seems the codes constructed in this way fall short of such comparison.

To describe the results, for the sake of clear presentation, we use the “modified” weight $\lambda(a, b)$, instead of the usual Hamming weight $w(\mathbf{c}_{(a,b)})$ for a codeword $\mathbf{c}_{(a,b)}$. The relation between them is given by the formula

$$(4) \quad w(\mathbf{c}_{(a,b)}) = \frac{h(r-1)}{q} - \lambda(a, b).$$

The case that $p \equiv 2 \pmod{3}$ is easy to describe.

Theorem 1. *Let $\mathcal{C}_{(q,m,h,e)}$ be the cyclic code defined by (2) and (3), and the parameters are given by (1) where $q = p^s$. Assume that $e = N = 3$ and $p \equiv 2 \pmod{3}$ (including the case $p = 2$).*

- (1). *If $3 \mid \frac{q-1}{h}$, the modified weight distribution of $\mathcal{C}_{(q,m,h,e)}$ is given by Table 1.*
- (2). *If $3 \nmid \frac{q-1}{h}$, the modified weight distribution of $\mathcal{C}_{(q,m,h,e)}$ is given by Table 2.*

TABLE 1. The case $e = N = 3$, $p \equiv 2 \pmod{3}$ and $3 \mid \frac{q-1}{h}$

Weight $\lambda(a, b)$	Frequency
$-\frac{h}{q} \{2(-1)^{ms/2} \sqrt{r} + 1\}$	$\frac{r-1}{27} \{r - 8 - 2(-1)^{ms/2} \sqrt{r}\}$
$\frac{h}{q} \{(-1)^{ms/2} \sqrt{r} - 1\}$	$\frac{2(r-1)}{27} \{4r - 14 + (-1)^{ms/2} \sqrt{r}\}$
$-\frac{h}{q} \{(-1)^{ms/2} \sqrt{r} + 1\}$	$\frac{2(r-1)}{9} \{r - 2 + (-1)^{ms/2} \sqrt{r}\}$
$-\frac{h}{q}$	$\frac{2(r-1)}{9} \{2r - 1 - (-1)^{ms/2} \sqrt{r}\}$
$\frac{h}{3q} \{r - 4(-1)^{ms/2} \sqrt{r} - 3\}$	$r - 1$
$\frac{h}{3q} \{r + 2(-1)^{ms/2} \sqrt{r} - 3\}$	$2(r - 1)$
$\frac{h(r-1)}{q}$	1

TABLE 2. The case $e = N = 3$, $p \equiv 2 \pmod{3}$, and $3 \nmid \frac{q-1}{h}$

Weight $\lambda(a, b)$	Frequency
$-\frac{h}{q} \{2(-1)^{ms/2} \sqrt{r} + 1\}$	$\frac{r-1}{27} \{r + 1 - 2(-1)^{ms/2} \sqrt{r}\}$
$\frac{h}{q} \{(-1)^{ms/2} \sqrt{r} - 1\}$	$\frac{2(r-1)}{27} \{4r - 5 + (-1)^{ms/2} \sqrt{r}\}$
$-\frac{h}{q} \{(-1)^{ms/2} \sqrt{r} + 1\}$	$\frac{2(r-1)}{9} \{r - 2 + (-1)^{ms/2} \sqrt{r}\}$
$-\frac{h}{q}$	$\frac{r-1}{9} \{4r - 11 - 2(-1)^{ms/2} \sqrt{r}\}$
$\frac{h}{3q} \{r + 2(-1)^{ms/2} \sqrt{r} - 3\}$	$r - 1$
$\frac{h}{3q} \{r - (-1)^{ms/2} \sqrt{r} - 3\}$	$2(r - 1)$
$\frac{h(r-1)}{q}$	1

Example 1. Let $p = 2, s = 2, q = 4, m = 3, r = 64, h = 1, e = N = 3$. Letting α be a generator of $\text{GF}(64)$ from Magma, which uses the irreducible polynomial

$x^6 + x^4 + x^3 + x + 1$, we can construct the code explicitly and the weight distribution of the cyclic code $\mathcal{C}_{(q,m,h,e)}$ is given by

$$1 + 63x^8 + 294x^{12} + 756x^{14} + 1890x^{16} + 1092x^{18}.$$

This is confirmed by computing Table 1, since $3 \mid \frac{q-1}{h} = 3$. Notice that there are only six weights because two of the weights in Table 1 are the same, namely,

$$-\frac{h(2(-1)^{ms/2}\sqrt{r} + 1)}{q} = \frac{h(r + 2(-1)^{ms/2}\sqrt{r} - 3)}{3q}.$$

Actually this happens if and only if $r = 2^6 = 64$. In other cases, there are always seven distinct weights.

This is a $[21, 6, 8]$ -cyclic code over $\text{GF}(4)$. Grassl's table shows that there is a $[21, 6, 12]$ code over $\text{GF}(4)$, and the best possible minimum distance is 12. \square

Example 2. Let $p = 2, s = 2, q = 4, m = 3, r = 64, e = h = 3, N = 3$. Letting α be a generator of $\text{GF}(64)$ from Magma, which uses the irreducible polynomial $x^6 + x^4 + x^3 + x + 1$, we can construct the code explicitly and the weight distribution of the cyclic code $\mathcal{C}_{(q,m,h,e)}$ is given by

$$1 + 126x^{30} + 252x^{36} + 756x^{42} + 1827x^{48} + 1134x^{54}.$$

This is confirmed by computing Table 2, since $3 \nmid \frac{q-1}{h} = 1$. Same as Example 1, there are only six weights because two of the weights in Table 2 are the same.

This is a $[63, 6, 30]$ -cyclic code over $\text{GF}(4)$. Grassl's table shows that there is a $[63, 6, 44]$ code over $\text{GF}(4)$, and the best possible minimum distance is 44. \square

The case that $p \equiv 1 \pmod{3}$ can be described but the results are a little more complicated, because they rely on a subtle choice of cubic characters of $\text{GF}(p)$ and $\text{GF}(r)$, which need to be made explicit. We list the results first and then explain how to compute them later.

Theorem 2. *Let $\mathcal{C}_{(q,m,h,e)}$ be the cyclic code defined by (2) and (3), and the parameters are given by (1) where $q = p^s$. Assume that $e = N = 3$ and $p \equiv 1 \pmod{3}$.*

- (1). *If $3 \mid \frac{q-1}{h}$, the modified weight distribution of $\mathcal{C}_{(q,m,h,e)}$ is given by Table 3.*
- (2). *If $3 \nmid \frac{q-1}{h}$, the modified weight distribution of $\mathcal{C}_{(q,m,h,e)}$ is given by Table 4.*

The symbols in Tables 3-4 are as follows: let

$$\omega := \frac{-1 + \sqrt{-3}}{2}.$$

Then there is a unique algebraic integer $\pi \in \mathbb{Z}[\omega]$ such that $\pi\bar{\pi} = p$ and $\pi \equiv -1 \pmod{3}$ ($\bar{\pi}$ is the complex conjugate of π), and we let ρ be the cubic character of $\text{GF}(r)$ arising from $(\frac{\cdot}{\pi})_3$, the standard cubic residue symbol of the ring $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, which is isomorphic to $\text{GF}(p)$, and the three Gaussian periods $\eta_1^{(3,r)}$, $\eta_\alpha^{(3,r)}$ and $\eta_{\alpha^2}^{(3,r)}$ are given by

$$\begin{aligned} \eta_1^{(3,r)} &= \frac{(-1)^{sm+1} r^{1/3} (\pi^{sm/3} + \bar{\pi}^{sm/3}) - 1}{3}, \\ \eta_\alpha^{(3,r)} &= \frac{(-1)^{sm+1} r^{1/3} (\rho^2(\alpha) \pi^{sm/3} + \rho(\alpha) \bar{\pi}^{sm/3}) - 1}{3}, \\ \eta_{\alpha^2}^{(3,r)} &= \frac{(-1)^{sm+1} r^{1/3} (\rho(\alpha) \pi^{sm/3} + \rho^2(\alpha) \bar{\pi}^{sm/3}) - 1}{3}. \end{aligned}$$

Moreover, the relation between the modified weight $\lambda(a, b)$ and the Hamming weight $w(\mathbf{c}_{(a,b)})$ is given by (4).

For computational purposes, we can choose the value of π explicitly. By the unique factorization property of the ring $\mathbb{Z}[\omega]$, the prime p can be represented as $p = a^2 - ab + b^2$ for some integers a, b . If, in addition, we require that $a \equiv 2 \pmod{3}$, $b \equiv 0 \pmod{3}$ and $b > 0$, then such integers a, b exist and are unique. We can choose $\pi = a + b\omega$. Hence $\bar{\pi} = a + b\omega^2 = (a - b) - b\omega$.

We still need to determine the value of $\rho(\alpha)$, which is either ω or ω^2 . This can be done by using the definition of $(\frac{\cdot}{\pi})_3$ and the explicit identification of $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$

with $\text{GF}(p)$ (see [6, Chapter 9]), and we can describe the algorithm as follows: since $p \nmid b$, there is an integer b' such that $bb' \equiv 1 \pmod{p}$. Let $N_{r/p} : \text{GF}(r) \rightarrow \text{GF}(p)$ be the norm map, we know that $N_{r/p}(\alpha) = \alpha^{(r-1)/(p-1)} \in \text{GF}(p)$, and $N_{r/p}(\alpha)$ can be naturally identified by an integer modulo p . It can be shown that either $N_{r/p}(\alpha)^{(p-1)/3} \equiv -b'a \pmod{p}$ or $N_{r/p}(\alpha)^{(p-1)/3} \equiv -1 + b'a \pmod{p}$. Then the value of $\rho(\alpha)$ is given by

$$\rho(\alpha) = \begin{cases} \omega & : \text{ if } N_{r/p}(\alpha)^{(p-1)/3} \equiv -b'a \pmod{p}, \\ \omega^2 & : \text{ if } N_{r/p}(\alpha)^{(p-1)/3} \equiv -1 + b'a \pmod{p}. \end{cases}$$

Example 3. Let $p = q = 7, s = 1, m = 3, h = 1, e = N = 3$. Letting α be a generator of $\text{GF}(7^3)$ from Magma, which uses the irreducible polynomial $x^3 + 6x^2 + 4$, we can construct the code explicitly and find that the weight distribution of the cyclic code $\mathcal{C}_{(q,m,h,e)}$ is

$$\begin{aligned} &1 + 342x^{30} + 342x^{32} + 342x^{36} + 3990x^{45} + 14364x^{46} + 12312x^{47} \\ &+ 16302x^{48} + 24624x^{49} + 14364x^{50} + 14364x^{51} + 12312x^{52} + 3990x^{54}. \end{aligned}$$

This is confirmed by computing Table 3, since $p \equiv 1 \pmod{3}$ and $3 \mid \frac{p-1}{h} = 6$. Here $7 = 2^2 - 2 * 3 + 3^2$, so $a = 2, b = 3, \pi = 2 + 3\omega$. We choose $b' = -2$ so that $bb' \equiv 1 \pmod{7}$. We find from Magma that $N_{r/p}(\alpha) = 3$. Hence $3^{(p-1)/3} = 3^2 \equiv 2 \pmod{7}$ and $-1 + ab' = -1 + 2 * (-2) = -5 \equiv 2 \pmod{7}$, so $\rho(\alpha) = \omega^2$. The Gaussian periods can be computed as $\eta_1^{(3,r)} = 2, \eta_\alpha^{(3,r)} = -12, \eta_{\alpha^2}^{(3,r)} = 9$. Now the weight distribution can be obtained from Table 3. There are only 13 weights because two of the weights in Table 3 are the same, namely

$$\frac{3h\eta_1^{(3,r)}}{q} = \frac{h(2\eta_{\alpha^2}^{(3,r)} + \eta_\alpha^{(3,r)})}{q} = \frac{18}{7}.$$

This is a $[57, 6, 30]$ -cyclic code over $\text{GF}(7)$. Grassl's table shows that there is a $[57, 6, 42]$ code over $\text{GF}(7)$, and the best possible minimum distance can not be larger than 45. \square

Example 4. Let $p = q = 7, s = 1, m = 3, e = h = 3, N = 3$. Letting α be a generator of $\text{GF}(7^3)$ from Magma, which uses the irreducible polynomial $x^3 + 6x^2 + 4$, we can construct the code explicitly and find that the weight distribution of the cyclic code $\mathcal{C}_{(q,m,h,e)}$ is

$$\begin{aligned} &1 + 342x^{93} + 342x^{99} + 342x^{102} + 4104x^{135} + 14364x^{138} + 12312x^{141} \\ &+ 16416x^{144} + 24282x^{147} + 14364x^{150} + 14364x^{153} + 12312x^{156} + 4104x^{162}. \end{aligned}$$

This is confirmed by computing Table 4, since $p \equiv 1 \pmod{3}$ and $3 \nmid \frac{q-1}{h} = 2$. As in Example 3, we find $\rho(\alpha) = \omega^2$, $\eta_1^{(3,r)} = 2$, $\eta_\alpha^{(3,r)} = -12$ and $\eta_{\alpha^2}^{(3,r)} = 9$. Now the weight distribution can be obtained from Table 4. Same as Example 3, there are only 13 weights because two of the weights in Table 4 are the same.

This is a $[171, 6, 93]$ -cyclic code over $\text{GF}(7)$. The length 171 of the code is too large for comparison with Grassl's table. \square

The ideas of the proofs of Theorems 1 and 2 are similar to those of [16], that is, first we use orthogonal properties of characters to transform the problem of finding the weight distribution into a problem of evaluating certain character sums over finite fields, and then we group character sums accordingly and relate them to counting the number of points on some curves over finite fields. For $e = N = 3$, the curves turn out to be elliptic curves, on which the number of points can be computed explicitly by using standard techniques involving Gauss sums and Jacobi sums. While the methods are similar, the problem in this paper is more complicated, because firstly $N = 3$, so there are three Gaussian periods instead of two; the difference is significant. Secondly, the prime p could be $p = 2$, $p \equiv 1 \pmod{3}$ and $p \equiv 2 \pmod{3}$, all of which need to be taken care of; moreover, whether or not 3

TABLE 3. The case $e = N = 3$, $p \equiv 1 \pmod{3}$, and $3 \mid \frac{q-1}{h}$

Weight $\lambda(a, b)$	Frequency
$\frac{3h}{q} \eta_1^{(3,r)}$	$\frac{r-1}{27} \{r - 8 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms})\}$
$\frac{3h}{q} \eta_\alpha^{(3,r)}$	$\frac{r-1}{27} \{r - 8 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms})\}$
$\frac{3h}{q} \eta_{\alpha^2}^{(3,r)}$	$\frac{r-1}{27} \{r - 8 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_1^{(3,r)} + \eta_\alpha^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho^2(\alpha)\pi^{ms} + \rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_1^{(3,r)} + \eta_{\alpha^2}^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_\alpha^{(3,r)} + \eta_1^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_\alpha^{(3,r)} + \eta_{\alpha^2}^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho^2(\alpha)\pi^{ms} + \rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_{\alpha^2}^{(3,r)} + \eta_1^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho^2(\alpha)\pi^{ms} + \rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q} \{2\eta_{\alpha^2}^{(3,r)} + \eta_\alpha^{(3,r)}\}$	$\frac{r-1}{9} \{r - 2 - (-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms})\}$
$-\frac{h}{q}$	$\frac{2(r-1)}{9} \{r + 1 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms})\}$
$\frac{h}{3q} \{r - 1 + 6\eta_1^{(3,r)}\}$	$r - 1$
$\frac{h}{3q} \{r - 1 + 6\eta_\alpha^{(3,r)}\}$	$r - 1$
$\frac{h}{3q} \{r - 1 + 6\eta_{\alpha^2}^{(3,r)}\}$	$r - 1$
$\frac{h(r-1)}{q}$	1

divides $\frac{q-1}{h}$ also has an effect. There are simply quite a few cases to consider and a lot of computation is involved. It turns out that the case $p = 2$ can be included into the case $p \equiv 2 \pmod{3}$.

The paper is organized as follows: in Section 2 we recall the result we obtained in [16] and apply it to the case $e = N = 3$; the cases $p = 2$ and p odd need to be taken care of separately; Section 3 is devoted to the proof of Theorem 2; in Section 4, we argue that $p = 2$ can be included into the case $p \equiv 2 \pmod{3}$, and we prove Theorem 1. We find the papers [10, 5, 15] quite inspiring and very well-written, which we use as general references and starting points of this paper. Interested

TABLE 4. The case $e = N = 3$, $p \equiv 1 \pmod{3}$, and $3 \nmid \frac{q-1}{h}$

Weight $\lambda(a, b)$	Frequency
$\frac{3h}{q}\eta_1^{(3,r)}$	$\frac{r-1}{27}\{r+1-(-1)^{ms}(\pi^{ms}+\bar{\pi}^{ms})\}$
$\frac{3h}{q}\eta_\alpha^{(3,r)}$	$\frac{r-1}{27}\{r+1-(-1)^{ms}(\pi^{ms}+\bar{\pi}^{ms})\}$
$\frac{3h}{q}\eta_{\alpha^2}^{(3,r)}$	$\frac{r-1}{27}\{r+1-(-1)^{ms}(\pi^{ms}+\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_1^{(3,r)}+\eta_\alpha^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho^2(\alpha)\pi^{ms}+\rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_1^{(3,r)}+\eta_{\alpha^2}^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho(\alpha)\pi^{ms}+\rho^2(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_\alpha^{(3,r)}+\eta_1^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho(\alpha)\pi^{ms}+\rho^2(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_\alpha^{(3,r)}+\eta_{\alpha^2}^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho^2(\alpha)\pi^{ms}+\rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_{\alpha^2}^{(3,r)}+\eta_1^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho^2(\alpha)\pi^{ms}+\rho(\alpha)\bar{\pi}^{ms})\}$
$\frac{h}{q}\{2\eta_{\alpha^2}^{(3,r)}+\eta_\alpha^{(3,r)}\}$	$\frac{r-1}{9}\{r-2-(-1)^{ms}(\rho(\alpha)\pi^{ms}+\rho^2(\alpha)\bar{\pi}^{ms})\}$
$-\frac{h}{q}$	$\frac{r-1}{9}\{2r-7-2(-1)^{ms}(\pi^{ms}+\bar{\pi}^{ms})\}$
$\frac{h}{q}\left(\frac{r-1}{3}+\eta_1^{(3,r)}+\eta_\alpha^{(3,r)}\right)$	$r-1$
$\frac{h}{q}\left(\frac{r-1}{3}+\eta_1^{(3,r)}+\eta_{\alpha^2}^{(3,r)}\right)$	$r-1$
$\frac{h}{q}\left(\frac{r-1}{3}+\eta_\alpha^{(3,r)}+\eta_{\alpha^2}^{(3,r)}\right)$	$r-1$
$\frac{h(r-1)}{q}$	1

readers may refer to them for some preliminary background and other information related to this subject.

Acknowledgment The author is grateful to the anonymous referees for many valuable suggestions which help improve the quality of the paper substantially, and to Professor Cunsheng Ding for bringing this problem to his attention.

2. PRELIMINARIES

We first prove that, given parameters $p, q, r, m, s, \beta, g, \dots$ etc with $r = q^m$ in (1) and conditions $h|(q-1)$ and $1 < e|\gcd(q-1, hm)$, the order of g is n , $(g\beta)^n = 1$ and the minimal polynomials of g^{-1} and $(\beta g)^{-1}$ are distinct over $\text{GF}(q)$ except when $q = 3, h = 1, e = m = 2$.

It is clear that the order of g is n . Since $q \equiv 1 \pmod{e}$ and

$$\frac{h(r-1)}{q-1} = h(q^{m-1} + \cdots + q + 1) \equiv hm \equiv 0 \pmod{e},$$

we also have $(g\beta)^n = 1$.

Now suppose that the minimal polynomials of g^{-1} and $(\beta g)^{-1}$ are the same over $\text{GF}(q)$, then there is an integer a , $0 \leq a \leq m-1$ such that

$$\frac{q-1}{h}(q^a-1) \equiv \frac{q^m-1}{e} \pmod{q^m-1}.$$

Clearly $a \neq 0$ as $e > 1$, so $a \geq 1$ and $m \geq 2$. Since

$$0 < \frac{q-1}{h}(q^a-1), \frac{q^m-1}{e} < q^m-1,$$

we have the equality

$$(5) \quad \frac{q-1}{h}(q^a-1) = \frac{q^m-1}{e}.$$

If $a \leq m-2$, then

$$\frac{(q-1)e}{h}(q^a-1) \leq q^2(q^{m-2}-1) = q^m - q^2 < q^m - 1,$$

so we must have $a = m-1$. From the equation (5) we find that

$$\frac{e(q-1)}{h} \left(\frac{q^{m-1}-1}{q-1} \right) = \frac{q^m-1}{q-1}.$$

Since

$$\gcd\left(\frac{q^{m-1}-1}{q-1}, \frac{q^m-1}{q-1}\right) = \frac{q^{\gcd(m-1, m)}-1}{q-1} = 1,$$

we obtain

$$q^{m-1}-1 = q-1 \implies m=2.$$

Hence

$$\frac{e(q-1)}{h} = q+1.$$

This implies that $e|(q-1, q+1) = (q-1, 2)$. Since $e > 1$, we have $e = 2$. Now from the above equation we find

$$q = \frac{2+h}{2-h}.$$

The only valid values are $h = 1$ and hence $q = 3$. So the minimal polynomials of g^{-1} and $(\beta g)^{-1}$ are distinct over $\text{GF}(q)$ except when $q = 3, h = 1, e = m = 2$. \square

Next we recall the general result we obtained in [16, Section 2].

Denote by $C^{(N,r)}$ the subgroup of $\text{GF}(r)^*$ generated by α^N . Since $N|(m, q-1)$, the integer $(r-1)/(q-1) = q^{m-1} + q^{m-2} + \cdots + q + 1$ is divisible by N , hence $\beta \in C^{(N,r)}$. It is also easy to see that $\text{GF}(q)^* \subset C^{(N,r)}$.

For any $u \in \text{GF}(r)$, define

$$(6) \quad \eta_u^{(N,r)} = \sum_{z \in C^{(N,r)}} \psi(zu),$$

where ψ is the canonical additive character of $\text{GF}(r)$, which is given by $\psi(x) = \exp\left(\frac{2\pi i}{p} \text{Tr}_p(x)\right)$, here Tr_p is the trace function from $\text{GF}(r)$ to $\text{GF}(p)$. Obviously $\eta_0^{(N,r)} = \frac{r-1}{N}$. If $u \neq 0$, the term $\eta_u^{(N,r)}$ is called a ‘‘Gaussian period’’. Note that the Gaussian periods $\eta_u^{(N,r)}$, $u \neq 0$ depend only on the particular coset of $\text{GF}(r)^*$ with respect to $C^{(N,r)}$ that u belongs to, so there are N such Gaussian periods.

Recall from [5, Lemma 5] (see also [10, 15]) that for any $(a, b) \in \text{GF}(r)^2$, the Hamming weight of the codeword $\mathbf{c}_{(a,b)}$ is given by

$$(7) \quad \omega(\mathbf{c}_{(a,b)}) = \frac{h(r-1)}{q} - \lambda(a, b),$$

where the ‘‘modified weight’’ $\lambda(a, b)$ is defined by

$$\lambda(a, b) = \frac{hN}{eq} \sum_{i=1}^e \eta_{(a+\beta^i b)g^i}^{(N,r)}.$$

It suffices to study $\lambda(a, b)$ only. We have proved in [16, Section 2] that $\lambda(a, b)$ can attain the following values.

Case 1. $\prod_{i=1}^e (a + \beta^i b) \neq 0$: For any $c_1, \dots, c_e \in \text{GF}(r)^*$, we write $\underline{c} = (c_1, \dots, c_e)$ and define

$$\mathcal{F}(\underline{c}) = \left\{ (a, b) \in \text{GF}(r)^2 : (a + \beta^i b) g^i c_i \in C^{(N, r)} \ \forall i \right\}.$$

Then

$$(8) \quad \lambda(a, b) = \frac{hN}{eq} \sum_{i=1}^e \eta_{c_i^{-1}}^{(N, r)}, \quad (a, b) \in \mathcal{F}(\underline{c})$$

$$(9) \quad f(\underline{c}) := \#\mathcal{F}(\underline{c}) = \frac{r-1}{N^e} \sum_{\substack{\chi_i^N = \epsilon \\ \chi_1, \dots, \chi_{e-1}}} f_{\chi_1, \dots, \chi_{e-1}}(\underline{c}),$$

where the sum is over all multiplicative characters χ_i 's of $\text{GF}(r)^*$ such that $\chi_i^N = \epsilon$, ϵ being the principal character, and

$$f_{\chi_1, \dots, \chi_{e-1}}(\underline{c}) = \prod_{i=1}^{e-1} \chi_i(g^i(1 - \beta^i)c_i c_e^{-1}) \sum_{b \in \text{GF}(r)} \prod_{i=1}^{e-1} \chi_i(b + \gamma_i),$$

$$(10) \quad \gamma_i = \frac{\beta^i}{1 - \beta^i}, \quad i = 1, 2, \dots, e-1.$$

Case 2. $(a, b) \neq (0, 0)$ and $a + \beta^t b = 0$ for some t , $1 \leq t \leq e$: Then

$$(11) \quad \lambda(-\beta^t b, b) = \frac{hN}{eq} \left\{ \frac{r-1}{N} + \sum_{\substack{i=1 \\ i \neq t}}^e \eta_{bg^i(\beta^i - \beta^t)}^{(N, r)} \right\}, \quad 1 \leq t \leq e.$$

3. THE CASE $e = N = 3$: THE GENERAL SETTING

When $e = N = 3$, the parameters are

$$\beta = \alpha^{(r-1)/3}, \quad g = \alpha^{(q-1)/h}, \quad 3 = \gcd\left(m, \frac{3(q-1)}{h}\right), \quad 3|h \text{ and } h|(q-1).$$

Hence $\beta^3 = 1, 1 + \beta + \beta^2 = 0$. Note that β and any $a \in \text{GF}(q)^*$ are both cubic powers in $\text{GF}(r)$. The exact values of the three Gaussian periods $\eta_u^{(e,r)}, u = 1, \alpha, \alpha^2$ are known ([13]), which we assume now.

3.1. Evaluation of $f(\underline{c})$. We fix a non-trivial cubic character ρ of $\text{GF}(r)^*$. Then all the cubic characters are ρ, ρ^2 and $\epsilon = \rho^3$. For $\underline{c} = (c_1, c_2, c_3)$ where $c_1, c_2, c_3 \in \text{GF}(r)^*$, from (8) and (9) we have

$$(12) \quad \lambda(a, b) = \frac{h}{q} \sum_{i=1}^3 \eta_{c_i^{-1}}^{(3,r)}, \quad (a, b) \in \mathcal{F}(\underline{c}),$$

$$(13) \quad f(\underline{c}) := \#\mathcal{F}(\underline{c}) = \frac{r-1}{3^3} \sum_{1 \leq e_1, e_2 \leq 3} \sum_{b \in \text{GF}(r)} \rho(f_1(b)^{e_1} f_2(b)^{e_2}),$$

where we define

$$f_1(b) = g(1 - \beta)c_1c_3^{-1}(b + \gamma_1), \quad f_2(b) = g^2(1 - \beta^2)c_2c_3^{-1}(b + \gamma_2).$$

Here $\gamma_i = \frac{\beta^i}{1-\beta^i}, 1 \leq i \leq 2$. We see that

$$\gamma_1 - \gamma_2 = \frac{\beta}{1 - \beta^2}.$$

For each e_1, e_2 , let $\underline{e} = (e_1, e_2)$. Define

$$\mathcal{A} = \{(e_1, e_2) : 1 \leq e_1, e_2 \leq 3\}, \quad \mathcal{A}_0 = \{(3, 3)\},$$

$$\mathcal{A}_1 = \{(3, 1), (3, 2), (3, 3)\}, \quad \mathcal{A}_2 = \{(1, 3), (2, 3), (3, 3)\},$$

$$\mathcal{A}_3 = \{(1, 2), (2, 1), (3, 3)\}, \quad \mathcal{A}_4 = \{(1, 1), (2, 2), (3, 3)\},$$

and

$$h_i(\underline{c}) := \sum_{\underline{e} \in \mathcal{A}_i} \sum_{b \in \text{GF}(r)} \rho(f_1(b)^{e_1} f_2(b)^{e_2}), \quad 0 \leq i \leq 4.$$

We can see that

$$(14) \quad f(\underline{c}) = \frac{r-1}{3^3} \left(h_1(\underline{c}) + h_2(\underline{c}) + h_3(\underline{c}) + h_4(\underline{c}) - 3h_0(\underline{c}) \right).$$

To compute $f(\underline{c})$, it suffices to compute $h_i(\underline{c})$ for each i . Since $\gamma_1 \neq \gamma_2$, we find

$$h_0(\underline{c}) = \sum_{\substack{b \in \text{GF}(r) \\ b + \gamma_i \neq 0}} 1 = r - 2.$$

As to $h_1(\underline{c})$, we have

$$h_1(\underline{c}) = \sum_{\substack{\underline{c} \in \mathcal{A}_1 \\ b + \gamma_1 \neq 0}} \sum_{b \in \text{GF}(r)} \rho^{e_2}(f_2(b)) = \sum_{b \in \text{GF}(r)} \sum_{e=1}^3 \rho^e(f_2(b)) - \sum_{e=1}^3 \rho^e(f_2(-\gamma_1)).$$

For any $x \in \text{GF}(r)$, define $\delta_3(x) = 1$ if $x \in \text{GF}(r)^*$ is a cubic power, and $\delta_3(x) = 0$ if otherwise. Then by the orthogonal property of characters we have

$$\delta_3(x) = \frac{1}{3} \sum_{e=1}^3 \rho^e(x), \quad x \in \text{GF}(r).$$

Using this we obtain

$$h_1(\underline{c}) = \#\{(y, b) : y^3 = f_2(b), y \neq 0\} - 3\delta_3(f_2(-\gamma_1)).$$

From this it is easy to check that

$$h_1(\underline{c}) = r - 1 - 3\delta_3(g^2 c_2 c_3^{-1}).$$

Then $h_2(\underline{c})$ is computed in a similar way. We obtain

$$h_2(\underline{c}) = r - 1 - 3\delta_3(g c_1 c_3^{-1}).$$

As for $h_3(\underline{c})$, we obtain

$$h_3(\underline{c}) = \sum_{e=1}^3 \sum_{b \in \text{GF}(r)} \rho^e(f_1(b)f_2(b)^2) = \sum_{e=1}^3 \sum_{\substack{b \in \text{GF}(r) \\ (b+\gamma_1)(b+\gamma_2) \neq 0}} \rho^e\left(\frac{f_1(b)}{f_2(b)}\right).$$

Make changes of variables we find

$$h_3(\underline{c}) = \sum_{e=1}^3 \sum_{\substack{b \in \text{GF}(r) \\ 1+(\gamma_1-\gamma_2)b \neq 0 \\ b \neq 0}} \rho^e\left(\frac{c_1}{g(1+\beta)c_2}(1+(\gamma_1-\gamma_2)b)\right).$$

Related to solving the equation

$$y^3 = \frac{c_1}{g(1+\beta)c_2}(1+(\gamma_1-\gamma_2)b), \quad (y, b) \in \text{GF}(r),$$

we find that

$$h_3(\underline{c}) = r - 1 - 3\delta_3(g^2c_1c_2^{-1}).$$

Finally we need to compute $h_4(\underline{c})$. We can write

$$h_4(\underline{c}) = \sum_{e=1}^3 \sum_{b \in \text{GF}(r)} \rho(c_1c_2c_3(b+\gamma_1)(b+\gamma_2)) = \sum_{e=1}^3 \sum_{b \in \text{GF}(r)} \rho(c_1c_2c_3b(b+\gamma_1-\gamma_2)).$$

Let A be the number of solutions $(y, b) \in \text{GF}(r)^2$ such that

$$(15) \quad C : y^3 = c_1c_2c_3b(b+\gamma_1-\gamma_2).$$

Then $h_4(\underline{c}) = A - 2$.

3.1.1. *Case 1: p odd.* If p is odd, we can make a change of variables to complete the squares on the right side of (15), so that the curve C is transformed into the elliptic curve

$$(16) \quad E : y^2 = x^3 - 3(c_1c_2c_3)^4.$$

The number of $\text{GF}(r)$ -points on E can be computed explicitly by using standard tools such as the Gauss sums and the Jacobi sums. For example, following the argument in [6, Theorem 4, p. 305] (see also [7, Exercise 21, p. 63]), we find that

$$A = r + \chi(-3)\rho(c_1c_2c_3)J(\rho, \rho) + \chi(-3)\overline{\rho(c_1c_2c_3)}\overline{J(\rho, \rho)},$$

where χ is the non-trivial quadratic character of $\text{GF}(r)^*$ and $J(\rho, \rho)$ is the Jacobi sum associated with the character ρ . The value $J(\rho, \rho)$ can be evaluated by the Hasse-Davenport relation and [6, Proposition 8.3.4]. The explicit result is a little complicated to state, because the choice of one of the two cubic characters ρ has a subtle influence on the exact value of $J(\rho, \rho)$, and $\rho(\alpha)$ could also be any of the two primitive cubic roots of the unity, depending on how we choose the generator α of $\text{GF}(r)^*$. However, the theory about it is well known, so we record the result as follows. Interested readers may refer to [6, Chapters 8,9,10] for details.

Lemma 1. *Let the assumptions be as before, $r = q^m, q = p^s, p$ odd. Let*

$$\omega := \frac{-1 + \sqrt{-3}}{2}.$$

Choosing ρ appropriately we have

$$J(\rho, \rho) = (-1)^{ms+1}\pi^{ms},$$

where

- 1). *If $p \equiv 1 \pmod{3}$, then $\pi \in \mathbb{Z}[\omega]$ is an algebraic integer such that $\pi\bar{\pi} = p$ and $\pi \equiv -1 \pmod{3}$. Identifying $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ with the finite field $\mathbb{F}_p \subset \mathbb{F}_r$, then ρ is the cubic character of \mathbb{F}_r^* arising from $(\frac{\cdot}{\pi})_3$, the standard cubic residue symbol in $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.*
- 2). *If $p \equiv 2 \pmod{3}$, then s is even and $\pi = \sqrt{-p}$. Identifying $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ with the finite field $\mathbb{F}_{p^2} \subset \mathbb{F}_r$, then ρ is the cubic character of \mathbb{F}_r^* arising from the standard cubic residue symbol in $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$.*

By Lemma 1 we obtain

$$A = r - \chi(-3)(-1)^{ms} \left(\rho(c_1 c_2 c_3) \pi^{ms} + \rho^2(c_1 c_2 c_3) \bar{\pi}^{ms} \right).$$

Therefore

$$h_4(\underline{c}) = r - 2 - \chi(-3)(-1)^{ms} \left(\rho(c_1 c_2 c_3) \pi^{ms} + \rho^2(c_1 c_2 c_3) \bar{\pi}^{ms} \right).$$

In summary we obtain

Lemma 2. *If p is odd, then for any $\underline{c} = (c_1, \dots, c_3)$ where $c_1, \dots, c_3 \in \text{GF}(r)^*$, we have*

$$\begin{aligned} f(\underline{c}) = & \frac{r-1}{3^3} \left(r + 1 - 3\delta_3(g^2 c_2 c_3^{-1}) - 3\delta_3(g c_1 c_3^{-1}) - 3\delta_3(g^2 c_1 c_2^{-1}) \right. \\ & \left. - \chi(-3)(-1)^{ms} \left(\rho(c_1 c_2 c_3) \pi^{ms} + \rho^2(c_1 c_2 c_3) \bar{\pi}^{ms} \right) \right). \end{aligned}$$

3.1.2. *Case 2: $p = 2$.* On this case, the characteristic of $\text{GF}(r)$ is 2. We find that

$$\gamma_1 - \gamma_2 = \frac{\beta}{1-\beta} - \frac{\beta^2}{1-\beta^2} = 1,$$

so the curve C given in (15) is

$$(17) \quad C : y^3 = c_1 c_2 c_3 b(b+1).$$

As in Section 2, ψ is the canonical additive character of $\text{GF}(r)$ given by $\psi(x) = \exp(\pi i \text{Tr}_2(x))$, here Tr_2 is the trace function from $\text{GF}(r)$ to $\text{GF}(2)$. It is easy to see that $x = b^2 + b$ for some $b \in \text{GF}(r)$ if and only if $\psi(x) = 1$, hence for any $a \in \text{GF}(r)$, the number of solutions for $b \in \text{GF}(r)$ such that $b^2 + b = a$ is $1 + \psi(a)$. So we find that the number of solutions $(y, b) \in \text{GF}(r)^2$ on the curve C in (17) is given by

$$A = \sum_{y \in \text{GF}(r)} 1 + \psi \left(\frac{y^3}{c_1 c_2 c_3} \right).$$

From this we obtain

$$A = r + 1 + 3\eta_{(c_1 c_2 c_3)^2}^{(3,r)}.$$

Therefore

$$h_4(\underline{c}) = A - 2 = r - 1 + 3\eta_{(c_1 c_2 c_3)^2}^{(3,r)}.$$

In summary we obtain

Lemma 3. *If $p = 2$, then for any $\underline{c} = (c_1, \dots, c_3)$ where $c_1, \dots, c_3 \in \text{GF}(r)^*$, we have*

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r + 2 + 3\eta_{(c_1 c_2 c_3)^2}^{(3,r)} - 3\delta_3(g^2 c_2 c_3^{-1}) - 3\delta_3(g c_1 c_3^{-1}) - 3\delta_3(g^2 c_1 c_2^{-1}) \right).$$

3.2. The remaining case. Next we need to evaluate $\lambda(-\beta^t b, b)$ in (11). For simplicity we adopt a notation: $\lambda \equiv \mu \pmod{\Delta}$ means that $\lambda, \mu \in \text{GF}(r)^*$ and $\frac{\lambda}{\mu}$ is a cube in $\text{GF}(r)^*$.

For $t = 1$, it is easy to see that

$$\beta^2 - \beta \equiv \beta^3 - \beta \equiv \beta - 1 \pmod{\Delta},$$

so we obtain

$$(18) \quad \lambda(-\beta b, b) = \frac{h}{q} \left\{ \frac{r-1}{3} + \eta_{bg^2(\beta-1)}^{(3,r)} + \eta_{b(\beta-1)}^{(3,r)} \right\}.$$

Similarly we find for $t = 2$

$$(19) \quad \lambda(-\beta^2 b, b) = \frac{h}{q} \left\{ \frac{r-1}{3} + \eta_{bg(\beta-1)}^{(3,r)} + \eta_{b(\beta-1)}^{(3,r)} \right\},$$

and for $t = 3$

$$(20) \quad \lambda(-\beta^3 b, b) = \frac{h}{q} \left\{ \frac{r-1}{3} + \eta_{bg(\beta-1)}^{(3,r)} + \eta_{bg^2(\beta-1)}^{(3,r)} \right\}.$$

4. THE CASE $e = N = 3$: $p \equiv 1 \pmod{3}$

It is known from (12) that the weight $\lambda(a, b)$ is a simple linear combination of the Gaussian periods. For $u \neq 0$, the Gaussian periods are

$$(21) \quad \eta_u^{(3,r)} = \begin{cases} \eta_1^{(3,r)} & \text{if } u \equiv 1 \pmod{\Delta}, \\ \eta_\alpha^{(3,r)} & \text{if } u \equiv \alpha \pmod{\Delta}, \\ \eta_{\alpha^2}^{(3,r)} & \text{if } u \equiv \alpha^2 \pmod{\Delta}. \end{cases}$$

The exact values of the three Gaussian periods are known ([13]), which we assume now and will make explicit later. Basically, when $p \equiv 1 \pmod{3}$, the three Gaussian periods are all distinct.

We summarize the argument as follows: each $c_i (\neq 0)$, $i = 1, 2, 3$ has three distinct values: $c_i \equiv 1, \alpha, \alpha^2 \pmod{\Delta}$, which result in three Gaussian periods $\eta_{c_i^{-1}}^{(3,r)}$, so $\lambda(a, b)$ from the equation (12) has at most 10 different values, and the value depends only on the vector $\underline{c} = (c_1, c_2, c_3)$ for which $(a, b) \in \mathcal{F}(\underline{c})$. Moreover, for each such vector \underline{c} , the number $\#\mathcal{F}(\underline{c}) = f(\underline{c})$ is given by Lemma 2. We also notice that when $p \equiv 1 \pmod{3}$, then $\left(\frac{-3}{p}\right) = 1$, here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol with respect to p , hence

$$\chi(-3) = \left(\frac{-3}{p}\right)^{ms} = 1.$$

The final results will depend on whether or not $3 \mid \frac{q-1}{h}$.

4.1. The Proof of Table 3. Assume first that $3 \mid \frac{q-1}{h}$, then $g = \alpha^{(q-1)/h}$ is a cube in $\text{GF}(r)$. By Lemma 2 we have

$$\begin{aligned} f(\underline{c}) &= \frac{r-1}{3^3} \left(r+1 - 3\delta_3(c_2c_3^{-1}) - 3\delta_3(c_1c_3^{-1}) - 3\delta_3(c_1c_2^{-1}) \right. \\ &\quad \left. - (-1)^{ms} (\rho(c_1c_2c_3)\pi^{ms} + \rho^2(c_1c_2c_3)\bar{\pi}^{ms}) \right). \end{aligned}$$

For any $u = 1, \alpha$ or α^2 , if $c_1 \equiv c_2 \equiv c_3 \equiv u \pmod{\Delta}$, then the “modified weight” $\lambda(a, b) = \frac{h}{q} 3\eta_{u-1}^{(3,r)} = \frac{3h}{q} \eta_{u-1}^{(3,r)}$, and the total number of such (a, b) ’s counted in this $\mathcal{F}(\underline{c})$ is given by

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r - 8 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms}) \right).$$

If c_1, c_2, c_3 are all distinct modulo Δ , then $\lambda(a, b) = \frac{h}{q} \left(\eta_1^{(3,r)} + \eta_\alpha^{(3,r)} + \eta_{\alpha^2}^{(3,r)} \right) = -\frac{h}{q}$, and the number of such (a, b) ’s counted in this $\mathcal{F}(\underline{c})$ is given by

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r + 1 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms}) \right).$$

The total number of such \underline{c} ’s is 6.

Let (i, j, k) be a permutation of $(1, 2, 3)$. If $c_i \equiv c_j \equiv 1 \pmod{\Delta}$ and $c_k \equiv \alpha \pmod{\Delta}$, then $\lambda(a, b) = \frac{h}{q} \left(2\eta_1^{(3,r)} + \eta_{\alpha^2}^{(3,r)} \right)$, and the number of such (a, b) ’s counted is given by

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r - 2 - (-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms}) \right).$$

The total number of such \underline{c} ’s is 3. On the other hand, if $c_i \equiv c_j \equiv 1 \pmod{\Delta}$ and $c_k \equiv \alpha^2 \pmod{\Delta}$, then $\lambda(a, b) = \frac{h}{q} \left(2\eta_1^{(3,r)} + \eta_\alpha^{(3,r)} \right)$, and the number of such (a, b) ’s counted is given by

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r - 2 - (-1)^{ms} (\rho^2(\alpha)\pi^{ms} + \rho(\alpha)\bar{\pi}^{ms}) \right).$$

The total number of such \underline{c} ’s is also 3.

Similarly we consider that cases that

- $c_i \equiv c_j \equiv \alpha \pmod{\Delta}$ and $c_k \equiv 1$ or $\alpha^2 \pmod{\Delta}$;
- $c_i \equiv c_j \equiv \alpha^2 \pmod{\Delta}$ and $c_k \equiv 1$ or $\alpha \pmod{\Delta}$;

and we can obtain similar results. This yields the first ten weights $\lambda(a, b)$ and the corresponding frequencies in Table 3.

We also need to count the weight $\lambda(a, b)$ and its frequency coming from (a, b) 's such that $a = -\beta^t b$ for some t , $1 \leq t \leq 3$. Such cases are treated in (18)–(20). Since $3 \mid \frac{q-1}{h}$, g is a cube in $\text{GF}(r)$. Considering $t = 1$ and $\lambda(-\beta b, b)$ in (18), we find that

$$\lambda(-\beta b, b) = \frac{h}{q} \left\{ \frac{r-1}{3} + 2\eta_{b(\beta-1)}^{(3,r)} \right\}.$$

This is $\frac{h}{q} \left\{ \frac{r-1}{3} + 2\eta_u^{(3,r)} \right\}$ with frequency $(r-1)/3$ for any $u = 1, \alpha, \alpha^2$ respectively when $b \in \text{GF}(r)^*$ varies. The results for $t = 2, 3$ are the same, and this yields the weights $\lambda(a, b)$ and frequencies from lines 11–13 in Table 3. The last line of Table 3 comes from $(a, b) = (0, 0)$, which corresponds to the codeword with Hamming weight zero. This completes the proof of Table 3. \square

4.2. The Proof of Table 4. Assume that $3 \nmid \frac{q-1}{h}$, so that $g \equiv \alpha$ or $\alpha^2 \pmod{\Delta}$. The analysis is similar in either case.

For any $u = 1, \alpha$ or α^2 , if $c_1 \equiv c_2 \equiv c_3 \equiv u \pmod{\Delta}$, then the “modified weight” $\lambda(a, b) = \frac{3h}{q}\eta_{u^{-1}}^{(3,r)}$, and the total number of such (a, b) 's counted in this $\mathcal{F}(\underline{c})$ is given by

$$f(\underline{c}) = \frac{r-1}{3^3} \left(r+1 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms}) \right).$$

If c_1, c_2, c_3 are all distinct modulo Δ , then $\lambda(a, b) = -\frac{h}{q}$, and the number of such (a, b) 's counted in this $\mathcal{F}(\underline{c})$ is given by

$$\begin{aligned} f(\underline{c}) = & \frac{r-1}{3^3} \left(r+1 - (-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms}) \right. \\ & \left. - 3\delta_3(g^2 c_2 c_3^{-1}) - 3\delta_3(g c_1 c_3^{-1}) - 3\delta_3(g^2 c_1 c_2^{-1}) \right). \end{aligned}$$

The total number of such \underline{c} 's is 6. Collecting all such \underline{c} 's into the set \mathcal{T}_1 , it is easy to check that

$$\sum_{\underline{c} \in \mathcal{T}_1} \delta_3(g^2 c_2 c_3^{-1}) = \sum_{\underline{c} \in \mathcal{T}_1} \delta_3(g c_1 c_3^{-1}) = \sum_{\underline{c} \in \mathcal{T}_1} \delta_3(g^2 c_1 c_2^{-1}) = 3.$$

Hence the total number of such (a, b) 's inside one of those $\mathcal{F}(\underline{c})$'s is given by

$$\sum f(\underline{c}) = \frac{r-1}{3^2} \left(2r - 7 - 2(-1)^{ms} (\pi^{ms} + \bar{\pi}^{ms}) \right).$$

Let (i, j, k) be a permutation of $(1, 2, 3)$. If $c_i \equiv c_j \equiv 1 \pmod{\Delta}$ and $c_k \equiv \alpha \pmod{\Delta}$, then $\lambda(a, b) = \frac{h}{q} \left(2\eta_1^{(3,r)} + \eta_{\alpha^2}^{(3,r)} \right)$, and the number of such (a, b) 's counted is given by

$$\begin{aligned} f(\underline{c}) = & \frac{r-1}{3^3} \left(r + 1 - \chi(-3)(-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms}) \right. \\ & \left. - 3\delta_3(g^2c_2c_3^{-1}) - 3\delta_3(gc_1c_3^{-1}) - 3\delta_3(g^2c_1c_2^{-1}) \right). \end{aligned}$$

The total number of such \underline{c} 's is 3. Collecting all such \underline{c} 's into the set \mathcal{T}_2 , it is easy to check that

$$\sum_{\underline{c} \in \mathcal{T}_2} \delta_3(g^2c_2c_3^{-1}) = \sum_{\underline{c} \in \mathcal{T}_2} \delta_3(gc_1c_3^{-1}) = \sum_{\underline{c} \in \mathcal{T}_2} \delta_3(g^2c_1c_2^{-1}) = 1.$$

Hence the total number of such (a, b) 's inside one of those $\mathcal{F}(\underline{c})$'s is given by

$$\sum f(\underline{c}) = \frac{r-1}{3^2} \left(r - 2 - (-1)^{ms} (\rho(\alpha)\pi^{ms} + \rho^2(\alpha)\bar{\pi}^{ms}) \right).$$

For all the other cases the results are similar. This yields the first 10 weights $\lambda(a, b)$ and the corresponding frequencies in Table 4.

We also need to count the weight $\lambda(a, b)$ and its frequency coming from (a, b) 's such that $a = -\beta^t b$ for some t , $1 \leq t \leq 3$. Such cases are treated in (18)–(20). Since $3 \nmid \frac{q-1}{h}$, g is not a cube in $\text{GF}(r)$. Considering $t = 1$ and $\lambda(-\beta b, b)$ in (18), we find that

$$\lambda(-\beta b, b) = \frac{h}{q} \left\{ \frac{r-1}{3} + \eta_{bg^2(\beta-1)}^{(3,r)} + \eta_{b(\beta-1)}^{(3,r)} \right\}.$$

The right hand side could be $\frac{h}{q} \left\{ \frac{r-1}{3} + \eta_1^{(3,r)} + \eta_{\alpha}^{(3,r)} \right\}$, $\frac{h}{q} \left\{ \frac{r-1}{3} + \eta_1^{(3,r)} + \eta_{\alpha^2}^{(3,r)} \right\}$ or $\frac{h}{q} \left\{ \frac{r-1}{3} + \eta_{\alpha}^{(3,r)} + \eta_{\alpha^2}^{(3,r)} \right\}$, each of which appears with frequency $(r-1)/3$ when $b \in$

$\text{GF}(r)^*$ varies. The results for $t = 2, 3$ are the same. This yields the weights $\lambda(a, b)$ and frequencies from lines 11–13 in Table 4. The last line of Table 4 comes from $(a, b) = (0, 0)$, which corresponds to the codeword with Hamming weight zero. This completes the proof of Table 4. \square

4.3. The Gaussian Periods. Finally we shall determine explicitly the three Gaussian periods $\eta_1^{(3,r)}$, $\eta_\alpha^{(3,r)}$ and $\eta_{\alpha^2}^{(3,r)}$. This could be provided by [13, Theorem 22], however, it seems the results do not distinguish the value $\eta_\alpha^{(3,r)}$ from $\eta_{\alpha^2}^{(3,r)}$, so we use the basic property [13, Proposition 1] to compute the values by ourselves. It works in general situation, but for simplicity, we stick to our notation and the special case that $e = N = 3$ and $p \equiv 1 \pmod{3}$.

First, for $k = 0, 1, 2$, define

$$G_k := \sum_{x \in \text{GF}(r)} \psi(\alpha^k x^3),$$

here as in Section 2, ψ is the canonical additive character of $\text{GF}(r)$. It is easy to see that

$$G_k = 3\eta_{\alpha^k}^{(3,r)} + 1, \quad k = 0, 1, 2.$$

So it is enough to find the values G_k . [13, (g) of Proposition 1] states the relation

$$G_k = \sum_{j=1}^2 \rho(\alpha)^{-jk} \tau(\rho^j),$$

where ρ is the cubic character of $\text{GF}(r)$ arising from $\chi_\pi(\cdot) := \left(\frac{\cdot}{\pi}\right)_3$ that we have chosen from Lemma 1, and for any multiplicative character ζ of $\text{GF}(r)$, $\tau(\zeta)$ is the Gauss sum given by

$$\tau(\zeta) := \sum_{x \in \text{GF}(r)^*} \zeta(x) \psi(x).$$

Because of the careful choice of π , we know that ([6, Section 4, Chapter 9])

$$J(\chi_\pi, \chi_\pi) = \pi, \quad \tau(\chi_\pi)^3 = p\pi,$$

where $J(\chi_\pi, \chi_\pi)$ and $\tau(\chi_\pi)$ are the Jacobi sum and Gauss sum defined on $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$, which is identified naturally as $\text{GF}(p)$. Since $r = p^{sm}$ and $3|sm$, by the Davenport-Hasse relation (see [6] or [13, Proposition 18]), we find that

$$\tau(\rho) = (-1)^{ms+1}(\tau(\chi_\pi))^{ms} = (-1)^{ms+1}(\tau(\chi_\pi)^3)^{ms/3} = (-1)^{ms+1}r^{1/3}\pi^{sm/3}.$$

We also derive

$$\tau(\rho^2) = \overline{\tau(\rho)} = (-1)^{ms+1}r^{1/3}\bar{\pi}^{sm/3}.$$

The values $\tau(\rho)$ and $\tau(\rho^2)$ can be used to evaluate G_k 's, which in turn provide explicit evaluations of $\eta_{\alpha^k}^{(3,r)}$'s as claimed in Theorem 2. Now the proof of Theorem 2 is complete. \square

5. THE CASE $e = N = 3$: $p \equiv 2 \pmod{3}$

5.1. We first argue that the cases $p = 2$ and $p \equiv 2 \pmod{3}$, p odd, can be brought together.

First, when $p \equiv 2 \pmod{3}$, whether p is odd or even, then $2|s$. The values of the Gaussian periods are described as follows.

Lemma 4 (Proposition 20, [13]). *Assume that $p \equiv 2 \pmod{3}$, $r = p^{sm}$, $6|sm$. Define*

$$G_u = 3\eta_u^{(3,r)} + 1, \quad u \in \text{GF}(r)^*.$$

Then

$$G_1 = -2(-1)^{ms/2}\sqrt{r}, \quad G_\alpha = G_{\alpha^2} = (-1)^{ms/2}\sqrt{r}.$$

So in either case, there are two distinct values in the Gaussian periods, and the formulas are the same.

Second, when $p \equiv 2 \pmod{3}$ and p is odd, then $\pi = \sqrt{-p}$. Since

$$\frac{r-1}{p-1} = p^{sm-1} + p^{sm-2} + \dots + p + 1 \equiv 0 \pmod{2},$$

and \mathbb{F}_p^* is generated by $\alpha^{(r-1)/(p-1)}$, any $a \in \mathbb{F}_p^*$ is a perfect square in $\text{GF}(r)$, hence $\chi(-3) = 1$. For any $\underline{c} = (c_1, c_2, c_3)$ where $c_1, c_2, c_3 \in \text{GF}(r)^*$, the formulas for $f(\underline{c})$ given by Lemma 2 can be simplified as

$$(22) \quad f(\underline{c}) = \begin{cases} \frac{r-1}{3^3} \left(r + 1 - 3\delta_3(g^2 c_2 c_3^{-1}) - 3\delta_3(g c_1 c_3^{-1}) - 3\delta_3(g^2 c_1 c_2^{-1}) \right. \\ \left. - (-1)^{ms/2} \sqrt{r} (\rho(c_1 c_2 c_3) + \rho^2(c_1 c_2 c_3)) \right). \end{cases}$$

Using

$$\rho(c_1 c_2 c_3) + \rho^2(c_1 c_2 c_3) = \begin{cases} 2 & \text{if } c_1 c_2 c_3 \in C^{(3,r)}, \\ -1 & \text{if } c_1 c_2 c_3 \notin C^{(3,r)}, \end{cases}$$

the formulas for $f(\underline{c})$ can be simplified further.

On the other hand, if $p = 2$, using the Gaussian periods described by Lemma 4, it is easy to find that for any $\underline{c} = (c_1, c_2, c_3)$ where $c_1, c_2, c_3 \in \text{GF}(r)^*$, the formula for $f(\underline{c})$ given by Lemma 3 is the same as the one for $f(\underline{c})$ given in (22). Therefore the results for $p = 2$ can be included into the case $p \equiv 2 \pmod{3}$.

5.2. The argument for $p \equiv 2 \pmod{3}$, p odd, is exactly the same as the previous section for $p \equiv 1 \pmod{3}$, and the results are summarized in Tables 3-4, except that we have to take into account of the extra conditions

$$\eta_\alpha^{(3,r)} = \eta_{\alpha^2}^{(3,r)}, \quad \eta_1^{(3,r)} + 2\eta_\alpha^{(3,r)} = -1.$$

In other words, some of the different weights in Table 3-4 turn out to be the same if $p \equiv 2 \pmod{3}$. Taking care of those repeated weights, we have completed the proof of Theorem 1.

REFERENCES

- [1] N. Boston, G. McGuire, *The weight distributions of cyclic codes with two zeros and zeta functions*, J. Symbolic Comput. **45** (2010), no. 7, 723–733.
- [2] A. Canteaut, P. Charpin, H. Dobbertin, *Weight divisibility of cyclic codes, highly nonlinear functions on F_{2^m} , and crosscorrelation of maximum-length sequences*, SIAM J. Discrete Math. **13** (2000), 105–138.
- [3] C. Carlet, P. Charpin, V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15** (1998), 125–156.
- [4] P. Charpin, *Cyclic codes with few weights and Niho exponents*, J. Combin. Theory Ser. A **108** (2004), no. 2, 247–259.
- [5] C. Ding, Y. Liu, C. Ma, L. Zeng, *The weight Distributions of the duals of cyclic codes with two zeros*, IEEE Trans. Inform. Theory **57** (2011), no. 12, 8000–8006.
- [6] K. Ireland, M. Rosen, “A classical introduction to modern number theory”, Second Edition, Graduate Texts in Mathematics **84**, Springer-Verlag, 1990.
- [7] N. Koblitz, “Introduction to elliptic curves and modular forms”, Graduate Texts in Mathematics **97**, Springer-Verlag, 1984.
- [8] J. Luo, K. Feng, *On the weight distributions of two classes of cyclic codes*, IEEE Trans. Inform. Theory **54** (2008), No. 12, 5332–5344.
- [9] J. Luo, Y. Tang, H. Wang, *On the weight distribution of a class of cyclic codes*, ISIT 2009, Seoul, Korea, June 28–July 3, 2009.
- [10] C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, *The weight Enumerator of a class of cyclic codes*, IEEE Trans. Inform. Theory **57** (2011), no. 1, 397–402.
- [11] G. McGuire, *On three weights in cyclic codes with two zeros*, Finite Fields Appl. **10** (2004), no. 1, 97–104.
- [12] M. Moisio, K. Ranto, *Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros*, Finite Fields Appl. **13** (2007), no. 4, 922–935.
- [13] G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith. **39** (1981), no. 3, 251–264.
- [14] R. Schoof, *Families of curves and weight distribution of codes*, Bull. Amer. Math. Soc. **32** (1995), no. 2, 171–183.

- [15] B. Wang, C. Tang, Y. Qi, Y. Yang, M. Xu, *The weight distributions of cyclic codes and elliptic curves*, to appear in IEEE Trans. Inform. Theory.
- [16] M. Xiong, *The weight distributions of a class of cyclic codes*, Finite Fields Appl. **18** (2012), no. 5, 933–945.
- [17] J. Yuan, C. Carlet, C. Ding, *The weight distribution of a class of linear codes from perfect nonlinear functions*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 712–717.

MAOSHENG XIONG: DEPARTMENT OF MATHEMATICS, HONG KONG UNIVERSITY OF SCIENCE
AND TECHNOLOGY, CLEAR WATER BAY, KOWLOON, HONG KONG

E-mail address: mamsxiong@ust.hk